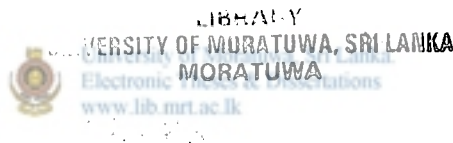


LB/DON/103/07

**BALANCED INTEGRATION OF INFORMATION
SECURITY INTO BUSINESS MANAGMENT
IN SRI LANKAN CONTEXT**

By

A.I.KALUARACHCHI



The Dissertation was submitted to the Department of Computer Science & Engineering of the University of Moratuwa in partial fulfilment of the requirement for the Degree of Master of Business Administration.

University of Moratuwa



89432

89432

Department of Computer Science & Engineering
University of Moratuwa

December 2006

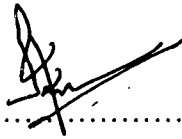
89432

004 - 06^y
004:65(043)

Declaration Form

I hereby declare that;

I have sincerely endeavoured to produce a research report of outstanding academic quality which will be useful to business organisations in understanding and deploying their information security management needs. The report presented is the sole work of my-self and none of this document is plagiarised (in whole or part) from any un-referenced outside source. I also certify that the work in this dissertation in part or whole has not been submitted for any other academic qualification at any institution.



.....
A.I. Kaluarachchi,

MBA/IT/03/9065

Department of Computer Science & Engineering

University of Moratuwa



University of Moratuwa, Sri Lanka
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

December 2006.

Certified by,



.....
Mr. Shantha Fernando

Supervisor.

Abstract

Today business are becoming more and more process based. Information is the basic building block of process based business. Organisations have to exchange massive amount of information with stakeholders in realising the business goals. Business needs information to be highly confidential in some aspects, where as in other aspects availability is the major.

The ultimate goal of information security is to reduce businesses risks associated with information exchange, storage and retrieval for stable functionality of a business. Securing information generated in business activities can not be isolated from the business practices; rather information security approach should be integrated into the management of business processes as an integral concern.

Most of the time information security is carried out by technical experts who try to make sure technical aspects of information security is taken care of. Non-technical aspects including human factors should be given due consideration to achieve better level of information security. Purposeful Information Security management needs a proper balance in several integration aspects.

Integration needs of information security and business management in Sri Lankan context are researched using multiple approaches in the thesis. Using the identified benefits and gaps it presents a model as well as recommendations for purposeful security dispatch in a business organization as a balanced, integrated approach with other business management practices.

Key words and phrases

Information, Information security, Business Management, Balanced Integration

Acknowledgement

This dissertation has been carried out in the Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka during the academic years 2004/2006. This study was for six months as a partial fulfilment of the Dissertation component of Master of Business Administration in Information Technology program.

Initially I wish to express my sincere gratitude to my supervisor, Mr Shantha Fernando for his inspiring support and counselling whenever called upon during the course of this study. Without his excellent guidance this work could not have reached completion.

I would also like to thank Ms Vishaka Nanayakkara-Head of the Department, all the examiners and panellists for this research and all other academic and non-academic staff members of the Computer Science & Engineering Department, University of Moratuwa, Sri Lanka who helped and guided me in numerous occasions.

I also express my sincere gratitude to Juhani Anttila and Jayalath L Jeewani for their support with experience in this research area. Without such support completing the present study would have been much harder.

My sincerest thanks are due to my family. Before all others, I wish to express my deepest gratitude to my wife Manori Welgama for her love and immense support throughout this research process. I also owe my special thanks to our wonderful son, Oshan Kaluarachchi.

Table of Contents

| | |
|---|------|
| DECLARATION FORM | II |
| ABSTRACT | III |
| ACKNOWLEDGEMENT..... | IV |
| TABLE OF CONTENTS | V |
| LIST OF FIGURES..... | VIII |
| LIST OF TABLES..... | X |
| CHAPTER 1 - INTRODUCTION | 1 |
| 1.1 BACKGROUND TO THE STUDY..... | 1 |
| 1.2 PROBLEM STATEMENT..... | 3 |
| 1.3 CONCEPTUAL FRAMEOWRK OF THE STUDY..... | 4 |
| 1.4 OBJECTIVES OF THE STUDY..... | 6 |
| 1.5 IMPORTANCE OF THE STUDY..... | 7 |
| 1.6 METHODOLOGY..... | 8 |
| 1.7 LIMITATIONS OF THE STUDY..... | 8 |
| CHAPTER 2 -LITERATURE VIEW..... | 9 |
| 2.1 INFORMATION NEEDS FOR A BUSINESS..... | 9 |
| 2.1.1 Information Life Cycle Management..... | 10 |
| 2.1.2 Information Sensitivity..... | 11 |
| 2.1.3 Information Systems and Information Technology | 13 |
| 2.2 INFORMATION SECURITY | 14 |
| 2.2.1 Layered Approach to Information Security..... | 17 |
| 2.2.2 Legal Framework on Information Security | 21 |
| 2.2.3 Information Security Standards..... | 22 |
| 2.2.4 Consequences of Information Security | 26 |
| 2.2.5 Survivability & Digital Forensics | 27 |
| 2.3 BUSINESS MANAGEMENT AND INFORMATION SECURITY..... | 29 |
| 2.3.1 Business Risk Analysis | 36 |
| 2.3.2 Security as a Core Competency | 38 |
| 2.4 SECURING BUSINESS INFORMATION | 38 |
| 2.4.1 Human Element of Information Security | 43 |
| 2.4.2 Employee Training on Information Security | 44 |
| 2.5 INTEGRATION OF INFORMATION SECURITY IN TO BUSINESS MANAGMENT..... | 45 |
| 2.5.1 Literature in Balanced Integration-Analysis..... | 53 |
| CHAPTER 3 - RESEARCH DESIGN & METHODOLOGY..... | 55 |
| 3.1 RESEARCH DESIGN & SCOPE | 55 |
| 3.2 SOURCES OF DATA & OPERATIONALIZATION..... | 56 |
| 3.3 RATIONAL OF THE RESERCH METHOD..... | 56 |
| 3.3.1 Structured Interview – Questioner..... | 56 |
| 3.3.2 Survey Questioner..... | 57 |

| | |
|--|-----|
| 3.3.3 Field Observations..... | 58 |
| 3.3.4 Internet Search..... | 59 |
| 3.5 METHOD OF ANALYSIS | 59 |
| CHAPTER 4 -DATA ANALYSIS AND FINDINGS | 60 |
| 4.1 STRUCTURED INTERVIEWS..... | 60 |
| 4.1.1 Significance of Information & Information Sharing Needs of a Business..... | 60 |
| 4.1.2 Business Information Security Needs..... | 61 |
| 4.1.3 Information Security – Who’s Responsibility | 62 |
| 4.1.4 Integration of Information Security & Business Management..... | 62 |
| 4.1.5 Benefits of Integrating Information Security & Business Management..... | 63 |
| 4.1.6 Barriers for Integration..... | 64 |
| 4.1.7 Analysis..... | 64 |
| 4.2 FIELD OBSERVATIONS..... | 65 |
| 4.2.1 Observation 01..... | 65 |
| 4.2.2 Observation 02..... | 66 |
| 4.2.3 Observation 03..... | 66 |
| 4.2.4 Observation 04..... | 67 |
| 4.2.5 Observation 05..... | 67 |
| 4.2.6 Observation 06..... | 67 |
| 4.2.7 Observation 07..... | 68 |
| 4.2.8 Analysis | 68 |
| 4.3 SURVEY QUESTIONNAIRE..... | 69 |
| 4.3.1 Overview of the Participant’s Organisations..... | 69 |
| 4.3.2 Information Security Awareness..... | 70 |
| 4.3.3 Need for Information Security..... | 74 |
| 4.3.4 Information Security..... | 77 |
| 4.3.5 Information Security & Business Management..... | 85 |
| 4.3.6 Perceptions on Information Security Measures..... | 91 |
| 4.4 INTERNET SEARCH..... | 96 |
| 4.4.1 CERT Statistics..... | 96 |
| 4.4.2 Information Security Breaches Survey 2006..... | 97 |
| 4.4.3 CSI/FBI Computer Crime and Security Survey, 2006. | 98 |
| 4.4.4 Global Information Security Survey 2005 | 99 |
| 4.4.5 Analyse..... | 102 |
| CHAPTER 5 - DISCUSSION OF FINDINGS..... | 104 |
| 5.1 BUSINESS NEEDS FOR INTERGATION WITH INFORMATION SECURITY..... | 105 |
| 5.2 INFORMATION SECURITY NEEDS FOR INTERGATION WITH BUSINESS MANAGEMENT..... | 108 |
| 5.3 INTERGATION GAPS..... | 110 |
| 5.4 DEMANDING FACTORS FOR ENHANCED INFORMATION SECURITY MANAGEMENT..... | 111 |
| 5.5 INFORMATION SECURITY REVIEW PROCESS..... | 112 |
| 5.6 INFORMATION SECURITY MANAGEMENT STRATRGIES..... | 113 |
| 5.7 BALANCED INTEGRATION OF INFORMATION SECURITY INTO BUSINESS MANAGEMENT..... | 114 |
| 5.8 BARRIERS FOR INTERGATION | 115 |

| | |
|--|-----|
| 5.9 BENEFITS OF INTERGATION..... | 116 |
| CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS..... | 117 |
| 6.1 CONCLUSION..... | 117 |
| 6.2 RECOMMENDATIONS..... | 119 |
| 6.3 SUGGESTIONS FOR FUTURE RESEARCHES..... | 120 |
| REFERENCES | 121 |
| APPENDIX | 126 |



University of Moratuwa, Sri Lanka
Electronic Theses & Dissertations
www.lib.mrt.ac.lk



List of Figures

| | |
|--|----|
| Figure 01 : Overall Cost of UK Companies Worst Case Incident in 2006..... | 02 |
| Figure 02 : Business Management Functions..... | 05 |
| Figure 03 : Hierarchy of Business Management..... | 05 |
| Figure 04 : Functional and Managerial Balance of Information Security..... | 06 |
| Figure 05 : Research Methodology..... | 08 |
| Figure 06 : Information Lifecycle..... | 11 |
| Figure 07 : Information Security is a Fuzzy Concept..... | 17 |
| Figure 08 : Information Security Management Implementation Process..... | 24 |
| Figure 09 : Collision of Specialised Management Areas..... | 30 |
| Figure 10 : Element of Business Management System..... | 31 |
| Figure 11 : Information Security Assurance..... | 32 |
| Figure 12 : Five Forces influence the organisation's objectives..... | 33 |
| Figure 13 : Strategic Alignment Model..... | 34 |
| Figure 14 : Goods and Information Flow in the Supply Chain..... | 35 |
| Figure 15 : Risk Assessment and Risk Management Process..... | 36 |
| Figure 16 : The Three Pillars of Purposeful Information Security Management..... | 52 |
| Figure 17 : Balanced Integration Model..... | 54 |
| Figure 18 : Research Design..... | 55 |
| Figure 19 : Primary Business of Survey Participants..... | 69 |
| Figure 20 : Staff Constitution of Surveyed Organisations..... | 70 |
| Figure 21 : Legal Framework Awareness..... | 71 |
| Figure 22 : Information Security Standards Awareness..... | 72 |
| Figure 23 : Staff Awareness on Information Security..... | 73 |
| Figure 24 : Top Management Awareness on Information Security..... | 74 |
| Figure 25 : Information and Communication Systems Utilized..... | 75 |
| Figure 26 : Significance of Information..... | 76 |
| Figure 27 : Responsibility of Information Security..... | 77 |
| Figure 28 : Security Measures Adopted..... | 78 |
| Figure 29 : Availability of Information Security Policy..... | 79 |
| Figure 30 : Security Policy Review Frequency..... | 80 |
| Figure 31 : Reported Information Security Breaches in Last Year..... | 81 |

| | |
|--|-----|
| Figure 32 : Consequences of Information Security Breaches..... | 82 |
| Figure 33 : Action Taken After Vulnerability..... | 83 |
| Figure 34 : Disaster Recovery Plan – Availability..... | 83 |
| Figure 35 : Business Continuity Plan – Availability..... | 84 |
| Figure 36 : Management Tools Adopted in Business..... | 85 |
| Figure 37 : Information Security as a Barrier to Business..... | 86 |
| Figure 38 : Information Security as a Barrier to Business – Perception..... | 87 |
| Figure 39 : Business Decisions as a Barrier to Information Security..... | 88 |
| Figure 40 : Business Decisions as a Barrier to Information Security – Perception.. | 88 |
| Figure 41 : Information Security Priority..... | 89 |
| Figure 42 : Information Security Risk Analysis Frequency..... | 90 |
| Figure 43 : Barriers for Information Security..... | 91 |
| Figure 44 : Information Security Measures Taken..... | 92 |
| Figure 45 : Information Security Measures Taken – Perception..... | 93 |
| Figure 46 : Perception of Existing DRP..... | 93 |
| Figure 47 : Perception of Existing BCP..... | 94 |
| Figure 48 : Perception of Present Information Security Implementation..... | 95 |
| Figure 49 : Number of Vulnerabilities Reported to CERT..... | 96 |
| Figure 50 : Security Breaches Reported | 97 |
| Figure 51 : Types of Attacks or Misuse detected in last 12 months..... | 99 |
| Figure 52 : Integration Requirements & Gaps Identification..... | 104 |
| Figure 53 : New Information Security Framework for Business..... | 112 |
| Figure 54 : Information Security Management Strategy Development..... | 113 |
| Figure 55 : Information Security Governs Information Systems..... | 116 |

List of Tables

| | | |
|----------|---|----|
| Table 01 | : OSI -The 7 Layer Architecture..... | 20 |
| Table 02 | : ISO 27000 Series..... | 25 |
| Table 03 | : Targets of Social Engineering attacks | 43 |
| Table 04 | : Primary Business Related to IT | 70 |



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk